Bull. Aust. Math. Soc. (First published online 2024), page 1 of 10*
doi:10.1017/S0004972724001047
*Provisional—final page numbers to be inserted when paper edition is published

ADDITIVE AND SUBTRACTIVE BASES OF $\mathbb{Z}_m$ IN AVERAGE

GUANGPING LIANG, YU ZHANG and HAODE ZUO

(Received 4 July 2024; accepted 1 October 2024)

Abstract

Given a positive integer m, let $\mathbb{Z}_m$ be the set of residue classes mod m. For $A \subseteq \mathbb{Z}_m$ and $n \in \mathbb{Z}_m$, let $\sigma_A(n)$ be the number of solutions to the equation $n = x + y$ with $x, y \in A$. Let $\mathcal{H}_m$ be the set of subsets $A \subseteq \mathbb{Z}_m$ such that $\sigma_A(n) \geq 1$ for all $n \in \mathbb{Z}_m$. Let

$$\ell_m = \min_{A \in \mathcal{H}_m} \Big\{ m^{-1} \sum_{n \in \mathbb{Z}_m} \sigma_A(n) \Big\}.$$

Ding and Zhao ['A new upper bound on Ruzsa's numbers on the Erdős–Turán conjecture', *Int. J. Number Theory* **20** (2024), 1515–1523] showed that $\limsup_{m\to\infty} \ell_m \leq 192$. We prove

$$\limsup_{m\to\infty} \ell_m \leq 144$$

and investigate parallel results on subtractive bases of $\mathbb{Z}_m$.

2020 *Mathematics subject classification*: primary 11B13; secondary 11B34.

Keywords and phrases: representation functions, Ruzsa's numbers, prime number theorem, additive bases.

1. Introduction

Let $\mathbb{N}$ be the set of natural numbers and A a subset of $\mathbb{N}$. A remarkable conjecture of Erdős and Turán [6] states that if all sufficiently large numbers n can be written as the sum of two elements of A, then the number of representations of n as the sum of two elements of A cannot be bounded. Progress on this conjecture was made by Grekos *et al.* [8], who proved that the number of representations cannot be bounded by 5, later improved to 7 by Borwein *et al.* [1]. For more on the Erdős–Turán conjecture, see the books of Halberstam and Roth [10] and Tao and Vu [17].

A set A is called an *asymptotic basis* of natural numbers if all sufficiently large numbers n can be written as the sum of two elements of A. Motivated by Erdős' question, Ruzsa [12] constructed an asymptotic basis A of natural numbers which has a bounded square mean value. Ruzsa also considered a variant on the Erdős–Turán conjecture. Let $\mathbb{Z}_m$ be the set of residue classes mod m and A a subset of $\mathbb{Z}_m$. For any

$n \in \mathbb{Z}_m$, let

$$\sigma_A(n) = \#\{(x, y) : n = x + y,\ x, y \in \mathbb{Z}_m\}.$$

The Ruzsa number R_m is defined to be the least positive integer r so that there exists a set $A \subseteq \mathbb{Z}_m$ with $1 \le \sigma_A(n) \le r$ for all $n \in \mathbb{Z}_m$. In his argument, Ruzsa proved that there is an absolute constant C such that $R_m \le C$ for all positive integers m. Employing Ruzsa's ideas, Tang and Chen [15] proved that $R_m \le 768$ for all sufficiently large m. Later, in [16], they obtained $R_m \le 5120$ for all positive integers m. In [2], Chen proved that $R_m \le 288$ for all positive integers m, and this was recently improved to $R_m \le 192$ by Ding and Zhao [5]. However, Sándor and Yang [13] showed that $R_m \ge 6$ for all $m \ge 36$.

Ding and Zhao [5] provided an average version of Ruzsa's number. Precisely, let $\mathcal{H}_m$ be the set of subsets $A \subseteq \mathbb{Z}_m$ such that $\sigma_A(n) \ge 1$ for all $n \in \mathbb{Z}_m$. Ding and Zhao defined the minimal mean value as

$$\ell_m = \min_{A \in \mathcal{H}_m} \Big\{ m^{-1} \sum_{n \in \mathbb{Z}_m} \sigma_A(n) \Big\}.$$

As they pointed out, their result on $R_m \le 192$ clearly implies

$$\limsup_{m \to \infty} \ell_m \le 192. \tag{1.1}$$

Ding and Zhao [5, Section 3] thought that '*any improvement of the bound (1.1) would be of interest*'. In this note, we shall make some progress on this problem.

THEOREM 1.1. *We have*

$$\limsup_{m \to \infty} \ell_m \le 144.$$

Parallel to the additive bases of $\mathbb{Z}_m$, one naturally considers the corresponding results on subtractive bases of $\mathbb{Z}_m$. Let A be a subset of $\mathbb{Z}_m$. For any $n \in \mathbb{Z}_m$, let

$$\delta_A(n) = \#\{(x, y) : n = x - y,\ x, y \in \mathbb{Z}_m\}.$$

In [3], Chen and Sun proved that for any positive integer m, there exists a subset A of $\mathbb{Z}_m$ so that $\delta_A(n) \ge 1$ for any $n \in \mathbb{Z}_m$ and $\delta_A(n) \le 7$ for all $n \in \mathbb{Z}_m$ with three exceptions. Their result was recently improved by Zhang [18] who showed that $\delta_A(n) \le 7$ could be refined to $\delta_A(n) \le 5$, again with three exceptions. The exceptions cannot be removed by their method. Motivated by the minimal mean value defined by Ding and Zhao, we consider a parallel quantity

$$g_m := \min_{A \in \mathcal{K}_m} \Big\{ m^{-1} \sum_{n \in \mathbb{Z}_m} \delta_A(n) \Big\},$$

where $\mathcal{K}_m$ is the set of subsets $A \subseteq \mathbb{Z}_m$ such that $\delta_A(n) \ge 1$ for all $n \in \mathbb{Z}_m$. Obviously, Zhang's bound implies that

$$\limsup_{m \to \infty} g_m \le 5$$

since the total sums of $\delta_A(n)$ for the three exceptions contribute only $O(\sqrt{m})$. Our second main result gives a small improvement on this bound.

THEOREM 1.2. *We have*

$$\limsup_{m\to\infty} g_m \le 2.$$

There is an old conjecture known as the *prime power conjecture* (see, for example, [7, 9, 11]) which states that if A is a subset of $\mathbb{Z}_m$ with $\delta_A(n) = 1$ for any nonzero $n \in \mathbb{Z}_m$, then $m = p^{2\alpha} + p^{\alpha} + 1$, where p^{α} is a prime power. The reverse direction was proved by Singer [14] as early as 1938.

As mentioned by Ding and Zhao [5], it is clear that $\liminf_{m\to\infty} \ell_m \ge 2$ from [13, Lemma 2.2]. They conjectured that $\liminf_{m\to\infty} \ell_m \ge 3$ [5, Conjecture 3.3]. Based on the results of Singer and Theorem 1.2, it seems reasonable to *conjecture* that

$$\lim_{m\to\infty} g_m = 1.$$

If true, these conjectures reflect rather different features between additive bases and subtractive bases.

2. Proof of Theorem 1.1

For any integer k, let

$$Q_k = \{(u, ku^2) : u \in \mathbb{Z}_p\} \subset \mathbb{Z}_p^2.$$

We will make use of the following lemmas.

LEMMA 2.1 (Chen [2, Lemma 2]). *Let p be an odd prime and m a quadratic nonresidue of p with $m + 1 \not\equiv 0 \pmod p$, $3m + 1 \not\equiv 0 \pmod p$ and $m + 3 \not\equiv 0 \pmod p$. Put*

$$B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}.$$

Then, for any $(c, d) \in \mathbb{Z}_p^2$, we have $1 \le \sigma_B(c, d) \le 16$, where $\sigma_B(c, d)$ is the number of solutions of the equation $(c, d) = x + y,\ x, y \in B$.

LEMMA 2.2 (Prime number theorem; see, for example, [4]). *Let $\pi(x)$ be the number of primes p not exceeding x. Then,*

$$\pi(x) \sim x/\log x \quad \text{as } x \to \infty.$$

LEMMA 2.3. *Let m be a positive integer and A a subset of $\mathbb{Z}_m$. Then,*

$$\sum_{n\in\mathbb{Z}_m} \sigma_A(n) = |A|^2,$$

where $|A|$ denotes the number of elements of A.

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

PROOF. Clearly,

$$\sum_{n\in\mathbb{Z}_m} \sigma_A(n) = \sum_{n\in\mathbb{Z}_m} \sum_{\substack{a_1+a_2=n \\ a_1,a_2\in A}} 1 = \sum_{\substack{a_1,a_2\in A \\ a_1+a_2\in\mathbb{Z}_m}} 1 = \sum_{a_1,a_2\in A} 1 = |A|^2.$$

This completes the proof of Lemma 2.3. □

LEMMA 2.4. *Let p be a prime greater than 11. Then there is a subset $A \subset \mathbb{Z}_{2p^2}$ with $|A| \le 12p$ so that $\sigma_A(n) \ge 1$ for any $n \in \mathbb{Z}_{2p^2}$.*

PROOF. Let p be a prime greater than 11. Then there are at least $(p-1)/2 > 5$ quadratic nonresidues mod p, which means that there is some quadratic nonresidue m so that

$$m + 1 \not\equiv 0 \pmod p, \quad 3m + 1 \not\equiv 0 \pmod p \quad \text{and} \quad m + 3 \not\equiv 0 \pmod p.$$

Let $B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}$, $A_1 = \{u + 2pv : (u, v) \in B\}$ and $A = A_1 \cup (A_1 + p)$, where $A_1 + p := \{a_1 + p : a_1 \in A_1\}$. Obviously, A can be viewed as a subset of $\mathbb{Z}_{2p^2}$.

We first show that $\sigma_A(n) \ge 1$ for any $n \in \mathbb{Z}_{2p^2}$, that is, $A \in \mathcal{H}_{2p^2}$ (by the definition of $\mathcal{H}_m$). We follow the proof of Chen [2, Theorem 1]. For any $(u, v) \in B$, we have $0 \le u, v \le p - 1$. Let n be an element of $\mathbb{Z}_{2p^2}$ with $0 \le n \le 2p^2 - 1$. Then, we can assume that

$$n = c + 2pd$$

with $p \le c \le 3p - 1$ and $-1 \le d \le p - 1$. By Lemma 2.1, there are $(u_1, v_1), (u_2, v_2) \in B$ so that

$$(c, d) = (u_1, v_1) + (u_2, v_2) \pmod p,$$

or in other words,

$$c \equiv u_1 + u_2 \pmod p \quad \text{and} \quad d \equiv v_1 + v_2 \pmod p.$$

Suppose that

$$c = u_1 + u_2 + ps \quad \text{and} \quad d = v_1 + v_2 + ph,$$

with $s, h \in \mathbb{Z}$. Then, $s = 0$ or 1 or 2 since $0 \le u_1 + u_2 \le 2p - 2$ and $p \le c \le 3p - 1$. Hence,

$$\begin{aligned} n &= c + 2pd \\ &= u_1 + 2pv_1 + u_2 + 2pv_2 + ps + 2p^2h \\ &\equiv u_1 + 2pv_1 + u_2 + 2pv_2 + ps \pmod{2p^2}. \end{aligned}$$

If $s = 0$, then in $\mathbb{Z}_{2p^2}$,

$$n = (u_1 + 2pv_1) + (u_2 + 2pv_2) \in A_1 + A_1 \subset A + A.$$

If $s = 1$, then in $\mathbb{Z}_{2p^2}$,

$$n = (u_1 + 2pv_1 + p) + (u_2 + 2pv_2) \in (A_1 + p) + A_1 \subset A + A.$$

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

If $s = 2$, then in $\mathbb{Z}_{2p^2}$,

$$n = (u_1 + 2pv_1 + p) + (u_2 + 2pv_2 + p) \in (A_1 + p) + (A_1 + p) \subset A + A.$$

Hence, in all cases, $\sigma_A(n) \geq 1$ for $n \in \mathbb{Z}_{2p^2}$.

It can be easily seen that $|A_1| \leq 2|B|$ from the construction. Therefore, for the set A constructed above,

$$|A| \leq |A_1| + |A_1 + p| = 2|A_1| \leq 2 \times 2|B| = 4|B|$$

and

$$|B| \leqslant |Q_{m+1}| + |Q_{m(m+1)}| + |Q_{2m}| = 3p,$$

from which it follows that

$$|A| \leq 12p.$$

This completes the proof of Lemma 2.4. $\square$

The final lemma gives a relation between the bases of $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{m_2}$ with certain constraints.

LEMMA 2.5. *Let $\varepsilon > 0$ be an arbitrarily small number. Let m_1 and m_2 be two positive integers with $(2 - \varepsilon)m_1 < m_2 < 2m_1$. If A is a subset of $\mathbb{Z}_{m_1}$ with $\sigma_A(n) \geq 1$ for any $n \in \mathbb{Z}_{m_1}$, then there is a subset B of $\mathbb{Z}_{m_2}$ with $|B| \leq 2|A|$ such that $\sigma_B(n) \geq 1$ for any $n \in \mathbb{Z}_{m_2}$.*

PROOF. Suppose that $m_2 = m_1 + r$, so that $(1 - \varepsilon)m_1 < r < m_1$. Let

$$B = A \cup \{a + r : a \in A\}.$$

Then, $|B| \leq 2|A|$. It remains to prove $\sigma_B(n) \geq 1$ for any $n \in \mathbb{Z}_{m_2}$.

Without loss of generality, we may assume $0 \leq a \leq m_1 - 1$ for any $a \in A$. For $0 \leq n \leq m_1 - 1$, there are two integers $a_1, a_2 \in A$ so that $n \equiv a_1 + a_2 \pmod{m_1}$. Since $0 \leq a_1 + a_2 \leq 2m_1 - 2$, it follows that

$$n = a_1 + a_2 \quad \text{or} \quad n = a_1 + a_2 - m_1.$$

If $n = a_1 + a_2$, then clearly $n \equiv a_1 + a_2 \pmod{m_2}$. If $n = a_1 + a_2 - m_1$, then

$$n + m_2 = n + m_1 + r = a_1 + (a_2 + r),$$

which means that $n \equiv a_1 + (a_2 + r) \pmod{m_2}$. In both cases, $\sigma_B(n) \geq 1$ for any n with $0 \leq n \leq m_1 - 1$. We are left to consider the case $m_1 \leq n \leq m_2 - 1$. In this range,

$$0 < n - r \leq m_2 - 1 - r = m_1 - 1.$$

Thus, there are two elements $\widetilde{a_1}, \widetilde{a_2}$ of A so that

$$n - r \equiv \widetilde{a_1} + \widetilde{a_2} \pmod{m_1}.$$

Again, by the constraint $0 \leq \widetilde{a_1} + \widetilde{a_2} \leq 2m_1 - 2$,

$$n - r = \widetilde{a_1} + \widetilde{a_2} \quad \text{or} \quad n - r = \widetilde{a_1} + \widetilde{a_2} - m_1.$$

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

If $n-r=\widetilde{a_1}+\widetilde{a_2}$, then we clearly have $n-r\equiv\widetilde{a_1}+\widetilde{a_2} \pmod{m_2}$. Otherwise, we have $n-r=\widetilde{a_1}+\widetilde{a_2}-m_1$. So, it can now be deduced that

$$n+m_2=\widetilde{a_1}+r+\widetilde{a_2}+r,$$

which is equivalent to $n\equiv(\widetilde{a_1}+r)+(\widetilde{a_2}+r) \pmod{m_2}$. □

PROOF OF THEOREM 1.1. Let $\varepsilon>0$ be an arbitrarily small given number. Then, by Lemma 2.2, there is some prime p so that

$$\sqrt{\frac{m}{4}}<p<\sqrt{\frac{m}{2(2-\varepsilon)}}, \tag{2.1}$$

provided that m is sufficiently large (in terms of ε). By Lemma 2.4, there is a subset $A\subset\mathbb{Z}_{2p^2}$ with $|A|\le 12p$ so that $\sigma_A(n)\ge 1$ for any $n\in\mathbb{Z}_{2p^2}$. From (2.1),

$$(2-\varepsilon)2p^2<m<2\times 2p^2. \tag{2.2}$$

Thus, by Lemma 2.5, there is a subset B of $\mathbb{Z}_m$ with

$$|B|\le 2|A|\le 24p \tag{2.3}$$

such that $\sigma_B(n)\ge 1$ for any $n\in\mathbb{Z}_m$. Hence, by Lemma 2.3,

$$\ell_m=\min_{\widetilde{A}\in\mathcal{H}_m}\Big\{m^{-1}\sum_{n\in\mathbb{Z}_m}\sigma_{\widetilde{A}}(n)\Big\}\le m^{-1}\sum_{n\in\mathbb{Z}_m}\sigma_B(n)=\frac{|B|^2}{m}.$$

Employing (2.2) and (2.3),

$$\frac{|B|^2}{m}\le\frac{(24p)^2}{(2-\varepsilon)2p^2}=144\times\frac{2}{2-\varepsilon}.$$

Hence, it follows that

$$\limsup_{m\to\infty}\ell_m\le 144\times\frac{2}{2-\varepsilon}$$

for any $\varepsilon>0$, which clearly means that

$$\limsup_{m\to\infty}\ell_m\le 144.$$

This completes the proof of Theorem 1.1. □

3. Proof of Theorem 1.2

The proof of Theorem 1.2 is based on the following remarkable result of Singer.

LEMMA 3.1 (Singer [14]). *Let p be a prime. Then, there exists a subset A of $\mathbb{Z}_{p^2+p+1}$ so that $\delta_A(n)=1$ for any $n\in\mathbb{Z}_{p^2+p+1}$ with $n\ne\overline{0}$.*

The next lemma is a variant of Lemma 2.3.

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

LEMMA 3.2. *Let m be a positive integer and A a subset of $\mathbb{Z}_m$. Then,*

$$\sum_{n\in\mathbb{Z}_m} \delta_A(n) = |A|^2,$$

where $|A|$ denotes the number of elements of A.

PROOF. It is clear that

$$\sum_{n\in\mathbb{Z}_m} \delta_A(n) = \sum_{n\in\mathbb{Z}_m} \sum_{\substack{a_1-a_2=n\\ a_1,a_2\in A}} 1 = \sum_{\substack{a_1,a_2\in A\\ a_1-a_2\in\mathbb{Z}_m}} 1 = \sum_{a_1,a_2\in A} 1 = |A|^2.$$

This completes the proof of Lemma 3.2. □

We need another auxiliary lemma.

LEMMA 3.3. *Let $\varepsilon > 0$ be an arbitrarily small number. Let m be a positive integer and p a prime number with*

$$(2-\varepsilon)(p^2+p+1) < m < 2(p^2+p+1).$$

If A is a subset of $\mathbb{Z}_{p^2+p+1}$ with $\delta_A(n) \geq 1$ for any $n \in \mathbb{Z}_{p^2+p+1}$, then there is a subset B of $\mathbb{Z}_m$ with $|B| \leq 2|A|$ such that $\delta_B(n) \geq 1$ for any $n \in \mathbb{Z}_m$.

PROOF. Suppose that $m = (p^2+p+1)+r$. Then, $(1-\varepsilon)(p^2+p+1) < r < (p^2+p+1)$. Let

$$B = A \cup \{a+r : a \in A\}.$$

Then, $|B| \leq 2|A|$. It remains to prove $\delta_B(n) \geq 1$ for any $n \in \mathbb{Z}_m$.

Without loss of generality, we can assume $0 \leq a \leq p^2+p$ for any $a \in A$. For $0 \leq n \leq p^2+p$, there are two integers $a_1, a_2 \in A$ so that

$$n \equiv a_1 - a_2 \pmod{p^2+p+1},$$

which means that

$$n = a_1 - a_2 \quad \text{or} \quad n = a_1 - a_2 + (p^2+p+1)$$

since $-p^2-p \leq a_1-a_2 \leq p^2+p$. If $n = a_1 - a_2$, then we clearly have $n \equiv a_1 - a_2 \pmod{m}$. If $n = a_1 - a_2 + (p^2+p+1)$, then

$$n - m = n - (p^2+p+1) - r = a_1 - (a_2 + r),$$

from which it can be deduced that $n \equiv a_1 - (a_2+r) \pmod{m}$. In both cases, we have $\delta_B(n) \geq 1$ for any n with $0 \leq n \leq p^2+p$. We are left to consider the case $p^2+p+1 \leq n \leq m-1$. In this case,

$$0 < n - r \leq m - 1 - r = p^2 + p.$$

Thus, there are two elements $\widetilde{a_1}, \widetilde{a_2}$ of A so that

$$n - r \equiv \widetilde{a_1} - \widetilde{a_2} \pmod{m}.$$

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

Again, by the constraint $-p^2 - p \le \widetilde{a_1} - \widetilde{a_2} \le p^2 + p$, we have

$$n - r = \widetilde{a_1} - \widetilde{a_2} \quad \text{or} \quad n - r = \widetilde{a_1} - \widetilde{a_2} + (p^2 + p + 1).$$

If $n - r = \widetilde{a_1} - \widetilde{a_2}$, then we clearly have $n - r \equiv \widetilde{a_1} - \widetilde{a_2} \pmod{m}$. Otherwise, we have $n - r = \widetilde{a_1} - \widetilde{a_2} + (p^2 + p + 1)$, from which it clearly follows that

$$n - m = \widetilde{a_1} - \widetilde{a_2}.$$

So we also deduce $n \equiv \widetilde{a_1} - \widetilde{a_2} \pmod{m}$. □

We now turn to the proof of Theorem 1.2.

Proof of Theorem 1.2. Let $\varepsilon > 0$ be an arbitrarily small given number. By Lemma 2.2, there is some prime p so that

$$\frac{\sqrt{2m-3}-1}{2} < p < \frac{\sqrt{\frac{4}{2-\varepsilon}m - 3} - 1}{2}$$

providing that m is sufficiently large (in terms of ε). Equivalently,

$$(2 - \varepsilon)(p^2 + p + 1) < m < 2(p^2 + p + 1). \tag{3.1}$$

By Lemma 3.1, there is a subset A of $\mathbb{Z}_{p^2+p+1}$ so that $\delta_A(n) = 1$ for any $n \in \mathbb{Z}_{p^2+p+1}$ with $n \ne \overline{0}$. Employing Lemma 3.2,

$$|A|^2 = \sum_{n \in \mathbb{Z}_{p^2+p+1}} \delta_A(n) = \sum_{n \in \mathbb{Z}_{p^2+p+1},\ n \ne \overline{0}} \delta_A(n) + \delta_A(0) = p^2 + p + |A|,$$

from which it follows clearly that

$$|A| = p + 1.$$

By Lemma 3.3 and (3.1), there is a subset B of $\mathbb{Z}_m$ with

$$|B| \le 2|A| \le 2(p + 1) \tag{3.2}$$

such that $\delta_B(n) \ge 1$ for any $n \in \mathbb{Z}_m$. Thus, by the definition of g_m and Lemma 3.2 again,

$$g_m = \min_{\widetilde{A} \in \mathcal{K}_m} \Big\{ m^{-1} \sum_{n \in \mathbb{Z}_m} \delta_{\widetilde{A}}(n) \Big\} \le m^{-1} \sum_{n \in \mathbb{Z}_m} \delta_B(n) = \frac{|B|^2}{m}.$$

From (3.1) and (3.2),

$$\frac{|B|^2}{m} \le \frac{4(p+1)^2}{(2-\varepsilon)(p^2+p+1)} \le \frac{4}{2 - \varepsilon/2},$$

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

provided that m (hence p) is sufficiently large (in terms of ε). Hence, we conclude that

$$\limsup_{m\to\infty} g_m \leq \frac{4}{2-\varepsilon/2}$$

for any $\varepsilon > 0$, which clearly means that

$$\limsup_{m\to\infty} g_m \leq 2.$$

This completes the proof of Theorem 1.2. □

Acknowledgement

The authors would like to thank Professor Yuchen Ding for his generous help and very helpful comments.

References

[1] P. Borwein, S. Choi and F. Chu, 'An old conjecture of Erdős–Turán on additive bases', *Math. Comp.* **75** (2006), 475–484.

[2] Y.-G. Chen, 'The analogue of Erdős–Turán conjecture in $\mathbb{Z}_m$', *J. Number Theory* **128** (2008), 2573–2581.

[3] Y.-G. Chen and T. Sun, 'The difference basis and bi-basis of $\mathbb{Z}_m$', *J. Number Theory* **130** (2010), 716–726.

[4] H. Davenport, *Multiplicative Number Theory*, 2nd edn, Graduate Texts in Mathematics, 74 (Springer-Verlag, New York, 1980).

[5] Y. Ding and L. Zhao, 'A new upper bound on Ruzsa's numbers on the Erdős–Turán conjecture', *Int. J. Number Theory* **20** (2024), 1515–1523.

[6] P. Erdős and P. Turán, 'On a problem of Sidon in additive number theory, and on some related problems', *J. Lond. Math. Soc. (2)* **16** (1941), 212–215.

[7] T. A. Evans and H. B. Mann, 'On simple difference sets', *Sankhyā* **11** (1951), 357–364.

[8] G. Grekos, L. Haddad, C. Helou and J. Pihko, 'On the Erdős–Turán conjecture', *J. Number Theory* **102** (2003), 339–352.

[9] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn, Problem Books in Mathematics, 1 (Springer-Verlag, New York, 2004).

[10] H. Halberstam and K. F. Roth, *Sequences* (Clarendon Press, Oxford, 1966).

[11] M. Hall Jr, 'Cyclic projective planes', *Duke Math. J.* **14** (1947), 1079–1090.

[12] I. Z. Ruzsa, 'A just basis', *Monatsh. Math.* **109** (1990), 145–151.

[13] C. Sándor and Q.-H. Yang, 'A lower bound of Ruzsa's number related to the Erdős–Turán conjecture', *Acta Arith.* **180** (2017), 161–169.

[14] J. Singer, 'A theorem in finite projective geometry and some applications to number theory', *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

[15] M. Tang and Y.-G. Chen, 'A basis of $\mathbb{Z}_m$', *Colloq. Math.* **104** (2006), 99–103.

[16] M. Tang and Y.-G. Chen, 'A basis of $\mathbb{Z}_m$, II', *Colloq. Math.* **108** (2007), 141–145.

[17] T. Tao and H. Van Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, 105 (Cambridge University Press, Cambridge, 2010).

[18] Y. Zhang, 'On the difference bases of $\mathbb{Z}_m$', *Period. Math. Hungar.*, to appear. Published online (10 July 2024).

GUANGPING LIANG, School of Mathematical Science,
Yangzhou University, Yangzhou 225002, PR China
e-mail: 15524259050@163.com

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press

YU ZHANG, School of Mathematics,
Shandong University, Jinan 250100, PR China
e-mail: yuzhang0615@mail.sdu.edu.cn

HAODE ZUO, School of Mathematical Science,
Yangzhou University, Yangzhou 225002, PR China
e-mail: yzzxzhd@yzu.edu.cn

https://doi.org/10.1017/S0004972724001047 Published online by Cambridge University Press